PCT/IB03/06166

#2

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03100033.4

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03100033.4
Demande no:

Anmeldetag:
Date of filing: 10.01.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH

20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Schaltungsanordnung und Verfahren zum Schutz elektronischer Bauelemente vor unzulässiger Manipulation und/oder vor unautorisiertem Zugriff

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F1/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR LI

BESCHREIBUNG

Schaltungsanordnung und Verfahren zum Schutz elektronischer Bauelemente vor unzulässiger Manipulation und/oder vor unautorisiertem Zugriff

Die vorliegende Erfindung betrifft das technische Gebiet des Schutzes elektronischer Bauelemente vor unzulässiger Manipulation und/oder vor unautorisiertem Zugriff.

Elektronische Bauelemente, die gegen unautorisierten Zugriff oder gegen unzulässige Veränderungen von Speicherinhalten geschützt werden sollen, werden konventionellerweise durch Aktivieren von Sicherungen (sogenannter "fuses") oder durch Speichern von Passwörtern verändert. Derartige Veränderungen werden bei Benutzung in der Prozedur des Aufstartens der eingebauten Zustandsmaschine (sogenannte "state machine") erkannt bzw. das gültige Passwort wird vor der Benutzung abgefragt und bestimmt dann die weitere Funktion; ebenso werden Sensoren, die den Versuch einer Manipulation eines Bauteils erkennen, in der Aufstartprozedur ausgewertet.

Diese vorstehend erläuterten Systeme gemäß dem Stand der Technik sind insofern nachteilig, als während der Aufstartprozedur selbst die Möglichkeit von Manipulationen gegeben ist; auch kann die Aufstartprozedur beliebig oft ausgeführt werden und somit selbst Gegenstand einer Analyse zum Zwecke der Manipulation werden.

Ausgehend von den vorstehend dargelegten Nachteilen und Unzulänglichkeiten sowie unter Würdigung des umrissenen Standes der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, eine mikroelektronische Schaltungsanordnung sowie ein Verfahren zum Schutz mindestens eines elektronischen Bauelements vor unzulässiger Manipulation und/oder vor unautorisiertem Zugriff bereitzustellen, bei denen auch während oder im Zusammenhang mit der Aufstartprozedur keinerlei Möglichkeiten zu Manipulationen bestehen.

Diese Aufgabe wird durch eine Schaltungsanordnung mit den im Anspruch 1 angegebenen Merkmalen sowie durch ein Verfahren mit den im Anspruch 5 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen und zweckmäßige Weiterbildungen der vorliegenden Erfindung sind in den Unteransprüchen gekennzeichnet.

Die mikroelektronische Schaltungsanordnung gemäß der vorliegenden Erfindung weist mehrere Einheiten oder Teile auf, wobei jeweils mindestens eine Aktivierungseinheit oder -schaltung und jeweils mindestens eine Verhinderungseinheit oder -schaltung zusammen vorhanden sind.

Die Aktivierungseinheit prüft das Vorliegen mindestens einer Aktivierungsbedingung ab und aktiviert im Falle mindestens einer erfüllten Aktivierungsbedingung (= unzulässige Manipulation und/oder unautorisierter Zugriff auf das elektronische Bauelement) die Verhinderungseinheit, mittels derer die Funktion des Bauelements zumindest partiell deaktivierbar und/oder das Bauelement zumindest partiell zerstörbar ist. In vorteilhafter Weise kann die Verhinderungseinheit in analoger Schaltungstechnik oder in mittelbar digitaler Schaltungstechnik (zum Beispiel "Fuse", "Antifuse") oder auch in gemischt analog/digitaler Schaltungstechnik ausgeführt sein.

Gemäß einer besonders erfinderischen Weiterbildung kann das Prüfen des Vorliegens mindestens einer Aktivierungsbedingung, das heißt das Erkennen der Startbedingung für die Selbstzerstörung durch Analyse eines von extern angelegten Datenstroms oder durch Signale der internen Sensorik bewerkstelligt werden.

Hinsichtlich der in der Aktivierungseinheit implementierten Aktivierungsmethoden bestehen mehrere unabhängig voneinander oder in Kombination miteinander realisierbare Optionen, so etwa

- das einmalige oder mehrfache Erkennen mindestens eines unzulässigen Befehls;
- das Erkennen mehrfacher unterschiedlicher unzulässiger Operationen;

- das Ansprechen mindestens eines bestimmten Aktivierungsbefehls;
- das Ansprechen mindestens eines Aktivierungsbefehls zusammen mit Daten, die mittels mindestens einer Gruppenerkennung mehrere Bauteile oder ein Bauteil mit individueller Kennung ansprechen; und/oder
- das einmalige oder mehrfache Erkennen mindestens eines physikalischen Angriffs auf das Bauelement mittels mindestens einer hierfür bestimmten Sensorik des Bauelements; unter einem "physikalischen Angriff" wird in diesem Zusammenhang beispielsweise
  - die Einwirkung von Licht,
  - eine Beschädigung einer Abdeckschicht des Bauelements oder
  - das Verlassen zulässiger Grenzwerte für die Frequenz und/oder für die Temperatur und/oder für die Versorgungsspannung oder für eine Kombination dieser Parameter

verstanden.

Hinsichtlich der in der Verhinderungseinheit implementierten Verhinderungsmethoden bestehen ebenfalls mehrere unabhängig voneinander oder in Kombination miteinander realisierbare Optionen, so etwa

- das Verhindern des Anschwingens mindestens eines internen Oszillators;
- das Verhindern des Anschwingens mindestens eines Oszillators für einen externen Takt;
- das Ausschalten mindestens einer Hochspannungsbegrenzung, insbesondere mittels dauernden Programmierens;
- das Verhindern des Aufbaus mindestens einer Hochspannung;
- das Umprogrammieren der Adresszuordnung und/oder der Datenzuordnung;
- das Belegen mindestens eines Speicherelements des Bauelements mit unzulässigen Datenwerten; und/oder
- das Einschalten mindestens einer erhöhten Stromaufnahme im Betriebszustand oder im Ruhezustand.

Zusammenfassend kann die vorliegende Erfindung also durch eine beispielsweise gemischt analog/digitale Schaltungsanordnung verwirklicht werden, die die Funktion des elektronischen Bauelements nach Aktivierung der Schaltungsanordnung durch erkannte externe Befehle oder durch interne Sensoren vorzugsweise irreversibel deaktiviert und/oder weitere Fehler auslöst.

Hierzu können unter Zuhilfenahme der zum Beispiel in E[lectrical]E[rasable] P[rogrammable]R[ead]O[nly]M[emory]- oder Flash-Produkten eingebauten Überwachungs- und Hochspannungsschaltungen zusätzlich zu konventionellen speicherbasierten "soft-fuses" weitere Fuses aktiviert werden, die den Betrieb des elektronischen Bauelements von Anfang an verhindern oder auch gewollte zusätzliche Folgefehler verursachen.

Hierdurch wird die Sicherheit der EEPROM- oder Flash-Produkte gegen Ausforschung und gegen Analyse gesteigert; des weiteren wird dem Kunden die Möglichkeit gegeben, sein Produkt im Feldeinsatz mit geeigneter Software gezielt zu deaktivieren bzw. irreversibel zu zerstören, sofern dem Kunden dies im Falle mindestens einer erfüllten Aktivierungsbedingung erforderlich erscheint.

In besonders zweckmäßiger Weise können die vorbeschriebenen Verknüpfungen in Verbindung mit sensorisch überwachten Abdeckschichten von EEPROM- oder Flash-Produkten dazu verwendet werden, diese nach partieller oder vollständiger Rückpräparation zu Analysezwecken zu zerstören.

Zusätzlich sind die vorbeschriebenen Funktionen insbesondere in S[mart] C[ard] C[ontroller]-Chips auch für den Endkunden interessant, denn dieser kann dann zum Beispiel gezielt im Feld befindliche Produkte bei Kontakt mit dem übergeordneten System deaktivieren.

Die vorliegende Erfindung betrifft schließlich die Verwendung mindestens einer Schaltungsanordnung gemäß der vorstehend dargelegten Art und/oder des Verfahrens gemäß der vorstehend dargelegten Art zum Selbstzerstören mindestens einer integrierten Schaltung beim unautorisierten Einsatz im Feld oder beim unzulässigen Versuch, die integrierte Schaltung durch zumindest partielle Rückpräparation zu analysieren.

Wie bereits vorstehend erörtert, gibt es verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Hierzu wird einerseits auf die dem Anspruch 1 sowie dem Anspruch 5 nachgeordneten Ansprüche verwiesen, andererseits werden weitere Ausgestaltungen, Merkmale und Vorteile der vorliegenden Erfindung nachstehend anhand des durch Figur 1 veranschaulichten Ausführungsbeispiels näher erläutert.

Es zeigt:

Fig. 1 in schematischer Darstellung ein Blockschaltbild eines Ausführungsbeispiels einer integrierten Schaltungsanordnung gemäß der vorliegenden Erfindung, die sich des Verfahrens gemäß der vorliegenden Erfindung bedient.

In Figur 1 ist ein Ausführungsbeispiel für eine zum Schutz eines elektronischen Bauelements 200 vor unzulässiger Manipulation und vor unautorisiertem Zugriff bestimmte mikroelektronische Schaltungsanordnung 100 dargestellt.

Grundsätzlich funktioniert diese Schaltungsanordnung 100 gemäß dem folgenden Arbeitsverfahren:

(i) Prüfen des Vorliegens einer Aktivierungsbedingung mittels der Aktivierungseinheiten A1, A2, A3, A4, A5, wobei

(i.1) die Aktivierungseinheit A1 zum einmaligen oder mehrfachen Erkennen eines unzulässigen Befehls,

(i.2) die Aktivierungseinheit A2 zum Erkennen mehrfacher unterschiedlicher unzulässiger Operationen,

(i.3) die Aktivierungseinheit A3 zum Ansprechen eines bestimmten Aktivierungsbefehls,

(i.4) die Aktivierungseinheit A4 zum Ansprechen eines Aktivierungsbefehls zusammen mit Daten, die mittels einer Gruppenerkennung mehrere Bauteile oder ein Bauteil mit individueller Kennung ansprechen, und/oder

(i.5) die Aktivierungseinheit A5 zum einmaligen oder mehrfachen Erkennen eines physikalischen Angriffs auf das Bauelement 200 mittels einer hierfür bestimmten Sensorik des Bauelements 200

ausgelegt ist;

(ii) im Falle einer erkannten unzulässigen Manipulation des Bauelements 200 und/oder eines erkannten unautorisierten Zugriffs auf das Bauelement 200: Aktivieren einer oder mehrerer mit den Aktivierungseinheiten A1, A2, A3, A4, A5 in Verbindung 110 stehender Verhinderungseinheiten V1, V2, V3, V4, V5, V6, V7, wobei

(ii.1) die Verhinderungseinheit V1 zum Verhindern des Anschwingens eines internen Oszillators,

(ii.2) die Verhinderungseinheit V2 zum Verhindern des Anschwingens eines Oszillators für einen externen Takt,

(ii.3) die Verhinderungseinheit V3 zum Ausschalten einer Hochspannungsbegrenzung, insbesondere mittels dauernden Programmierens,

(ii.4) die Verhinderungseinheit V4 zum Verhindern des Aufbaus einer Hochspannung,

(ii.5) die Verhinderungseinheit V5 zum Umprogrammieren der Adresszuordnung und der Datenzuordnung,

(ii.6) die Verhinderungseinheit V6 zum Belegen des Speicherelements 210 des Bauelements 200 mit unzulässigen Datenwerten und/oder

(ii.7) die Verhinderungseinheit V7 zum Einschalten einer erhöhten Stromaufnahme im Betriebszustand oder im Ruhezustand

ausgelegt ist; und

(iii) Deaktivieren der Funktion des Bauelements 200 und/oder Zerstören des Bauelements 200 mittels der Verhinderungseinheiten V1, V2, V3, V4, V5, V6, V7.

Das in Figur 1 dargestellte Ausführungsbeispiel basiert nun im speziellen auf dem Prinzip der Deaktivierung der Hochspannung:

Bei Vorliegen der Aktivierungsbedingung, das heißt bei Erkennung der Startbedingung für die Selbstzerstörung - sei es durch Analyse eines von extern angelegten Datenstroms oder durch Signale der internen Sensorik des Bauelements 200 - werden diese Erkenntnis sowie die erwünschten Auswirkungen kodiert und in dem beim Aufstarten verwendeten Speicher 210 hinterlegt, nämlich in Form der Selbstzerstörung SZ sowie der Verhinderungsmethoden V1, V2, V4, V7.

Im nächsten Schritt wird die Aufstartprozedur wiederholt, die bei Erkennen der Bedingung für die Selbstzerstörung SZ die entsprechenden Aktionen initiiert.

Beim nächsten Versuch des Aufstartens des Produkts ergeben sich dann folgende Bedingungen:

[a] Auslesen der Bedingungen;

[b] Verhinderungsmethode V7 gesetzt:
Einschalten erhöhter Stromaufnahme;

[c] Verhinderungsmethode V4 gesetzt:
Blockieren der Erzeugung von Hochspannung;

[d] Verhinderungsmethode V2 gesetzt:
Ignorieren des externen Takts;

[e] Verhinderungsmethode V1 gesetzt:
Anhalten des internen Takts.

Demzufolge können verschiedene Zustände zwischen vollständiger Funktionslosigkeit des Bauelements 200, Einschränkung des Funktionsumfangs des Bauelements 200 (etwa kein Programmieren mehr) bis hin zu absichtlichen Störungen des Umfelds der integrierten Schaltung (etwa erhöhter Ruhestrom zum Beispiel für batteriebetriebene Anwendungen) bewirkt werden.

BEZUGSZEICHENLISTE

100	mikroelektronische Schaltungsanordnung
110	Verbindung zwischen Aktivierungseinheiten Ai (i = 1, 2, 3, 4, 5) und Verhinderungseinheiten Vj (j = 1, 2, 3, 4, 5, 6, 7)
200	elektronisches Bauelement
210	Speicherelement des Bauelements 200
A1	erste Aktivierungseinheit oder erste Aktivierungsmethode
A2	zweite Aktivierungseinheit oder zweite Aktivierungsmethode
A3	dritte Aktivierungseinheit oder dritte Aktivierungsmethode
A4	vierte Aktivierungseinheit oder vierte Aktivierungsmethode
A5	fünfte Aktivierungseinheit oder fünfte Aktivierungsmethode
SZ	Selbstzerstörung
V1	erste Verhinderungseinheit oder erste Verhinderungsmethode
V2	zweite Verhinderungseinheit oder zweite Verhinderungsmethode
V3	dritte Verhinderungseinheit oder dritte Verhinderungsmethode
V4	vierte Verhinderungseinheit oder vierte Verhinderungsmethode
V5	fünfte Verhinderungseinheit oder fünfte Verhinderungsmethode
V6	sechste Verhinderungseinheit oder sechste Verhinderungsmethode
V7	siebte Verhinderungseinheit oder siebte Verhinderungsmethode

PATENTANSPRÜCHE

1. Zum Schutz mindestens eines elektronischen Bauelements (200) vor unzulässiger Manipulation und/oder vor unautorisiertem Zugriff bestimmte mikroelektronische Schaltungsanordnung (100), aufweisend mindestens eine Aktivierungseinheit (Ai; i = 1, 2, 3, 4, 5) zum Prüfen des Vorliegens mindestens einer Aktivierungsbedingung und zum Aktivieren mindestens einer der Schaltungsanordnung (100) ebenfalls zugeordneten, mit der Aktivierungseinheit (Ai) in Verbindung (110) stehenden Verhinderungseinheit (Vj; j = 1, 2, 3, 4, 5, 6, 7), mittels derer im Falle einer unzulässigen Manipulation und/oder eines unautorisierten Zugriffs das Bauelement (200) zumindest partiell deaktivierbar und/oder zumindest partiell zerstörbar ist.

2. Schaltungsanordnung gemäß Anspruch 1,
dadurch gekennzeichnet,
dass die Verhinderungseinheit (Vj)

- in analoger Schaltungstechnik oder
- in zumindest mittelbar digitaler Schaltungstechnik, zum Beispiel als mindestens ein Fuse und/oder als mindestens ein Antifuse,

ausgebildet ist.

3. Schaltungsanordnung gemäß Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass die Aktivierungseinheit (Ai)

(i = 1) zum einmaligen oder mehrfachen Erkennen mindestens eines unzulässigen Befehls;

(i = 2) zum Erkennen mehrfacher unterschiedlicher unzulässiger Operationen;

(i = 3) zum Ansprechen mindestens eines bestimmten Aktivierungsbefehls;

(i = 4) zum Ansprechen mindestens eines Aktivierungsbefehls zusammen mit Daten, die mittels mindestens einer Gruppenerkennung mehrere Bauteile oder ein Bauteil mit individueller Kennung ansprechen; und/oder

(i = 5) zum einmaligen oder mehrfachen Erkennen mindestens eines physikalischen Angriffs auf das Bauelement (200) mittels mindestens einer hierfür bestimmten Sensorik des Bauelements (200)

ausgelegt ist.

4. Schaltungsanordnung gemäß mindestens einem der Ansprüche 1 bis 3, dadurch gekennzeichnet,

dass die Verhinderungseinheit (Vj)

(j = 1) zum Verhindern des Anschwingens mindestens eines internen Oszillators;

(j = 2) zum Verhindern des Anschwingens mindestens eines Oszillators für einen externen Takt;

(j = 3) zum Ausschalten mindestens einer Hochspannungsbegrenzung, insbesondere bei kontinuierlichem Programmieren;

(j = 4) zum Verhindern des Aufbaus mindestens einer Hochspannung;

(j = 5) zum Umprogrammieren der Adresszuordnung und/oder der Datenzuordnung;

(j = 6) zum Belegen mindestens eines Speicherelements (210) des Bauelements (200) mit unzulässigen Datenwerten; und/oder

(j = 7) zum Einschalten mindestens einer erhöhten Stromaufnahme im Betriebszustand oder im Ruhezustand

ausgelegt ist.

5. Verfahren zum Schutz mindestens eines elektronischen Bauelements (200) vor unzulässiger Manipulation und/oder vor unautorisiertem Zugriff,
gekennzeichnet durch
die folgenden Verfahrensschritte:

(i) Prüfen des Vorliegens mindestens einer Aktivierungsbedingung mittels mindestens einer Aktivierungseinheit (Ai; i = 1, 2, 3, 4, 5);

(ii) im Falle einer unzulässigen Manipulation des Bauelements (200) und/oder eines unautorisierten Zugriffs auf das Bauelement (200):
Aktivieren mindestens einer mit der Aktivierungseinheit (Ai) in Verbindung (110) stehenden Verhinderungseinheit (Vj; j = 1, 2, 3, 4, 5, 6, 7); und

(iii) zumindest partielles Deaktivieren der Funktion des Bauelements (200) und/oder zumindest partielles Zerstören des Bauelements (200) mittels der Verhinderungseinheit (Vj).

6. Verfahren gemäß Anspruch 5,
dadurch gekennzeichnet,
dass das Vorliegen der Aktivierungsbedingung

- mittels Analysieren mindestens eines von extern angelegten Datenstroms oder
- durch Signale der internen Sensorik des Bauelements (200)

geprüft wird.

7. Verfahren gemäß Anspruch 5 oder 6,
dadurch gekennzeichnet,
dass bei Vorliegen der Aktivierungsbedingung

- diese Erkenntnis (A1, A2, A3, A4, A5) sowie die erwünschten Auswirkungen (V1, V2, V3, V4, V5, V6, V7) kodiert und in mindestens einem beim Aufstarten des Bauelements (200) verwendeten Speicherelement (210) hinterlegt werden und
- das die entsprechenden Aktionen initiierende Aufstarten wiederholt wird.

8. Verfahren gemäß mindestens einem der Ansprüche 5 bis 7,
dadurch gekennzeichnet,
dass das Aktivieren

(i = 1) durch einmaliges oder mehrfaches Erkennen mindestens eines unzulässigen Befehls;

(i = 2) durch Erkennen mehrfacher unterschiedlicher unzulässiger Operationen;

(i = 3) durch Ansprechen mindestens eines bestimmten Aktivierungsbefehls;

(i = 4) durch Ansprechen mindestens eines Aktivierungsbefehls zusammen mit Daten, die mittels mindestens einer Gruppenerkennung mehrere Bauteile oder ein Bauteil mit individueller Kennung ansprechen; und/oder

(i = 5) durch einmaliges oder mehrfaches Erkennen mindestens eines physikalischen Angriffs auf das Bauelement (200) mittels mindestens einer hierfür bestimmten Sensorik des Bauelements (200)

erfolgt.

9. Verfahren gemäß mindestens einem der Ansprüche 5 bis 8,
dadurch gekennzeichnet,
dass das zumindest partielle Deaktivieren der Funktion des Bauelements (200) und/oder das zumindest partielle Zerstören des Bauelements (200)

(j = 1) durch Verhindern des Anschwingens mindestens eines internen Oszillators;

(j = 2) durch Verhindern des Anschwingens mindestens eines Oszillators für einen externen Takt;

(j = 3) durch Ausschalten mindestens einer Hochspannungsbegrenzung, insbesondere bei kontinuierlichem Programmieren;

(j = 4) durch Verhindern des Aufbaus mindestens einer Hochspannung;

(j = 5) durch Umprogrammieren der Adresszuordnung und/oder der Datenzuordnung;

(j = 6) durch Belegen mindestens eines Speicherelements (210) des Bauelements (200) mit unzulässigen Datenwerten; und/oder

(j = 7) durch Einschalten mindestens einer erhöhten Stromaufnahme im Betriebszustand oder im Ruhezustand

erfolgt.

10. Verwendung mindestens einer Schaltungsanordnung (100) gemäß mindestens einem der Ansprüche 1 bis 4 und/oder des Verfahrens gemäß mindestens einem der Ansprüche 5 bis 9 zum Selbstzerstören mindestens einer integrierten Schaltung beim unautorisierten Einsatz im Feld oder beim unzulässigen Versuch, die integrierte Schaltung durch zumindest partielle Rückpräparation zu analysieren.

ZUSAMMENFASSUNG

Schaltungsanordnung und Verfahren zum Schutz elektronischer Bauelemente vor unzulässiger Manipulation und/oder vor unautorisiertem Zugriff

Um eine mikroelektronische Schaltungsanordnung (100) sowie ein Verfahren zum Schutz mindestens eines elektronischen Bauelements vor unzulässiger Manipulation und/oder vor unautorisiertem Zugriff bereitzustellen, bei denen auch während oder im Zusammenhang mit der Aufstartprozedur keinerlei Möglichkeiten zu Manipulationen bestehen, wird vorgeschlagen, mindestens eine Aktivierungseinheit (Ai; i = 1, 2, 3, 4, 5) zum Prüfen des Vorliegens mindestens einer Aktivierungsbedingung und zum Aktivieren mindestens einer der Schaltungsanordnung (100) ebenfalls zugeordneten, mit der Aktivierungseinheit (Ai) in Verbindung (110) stehenden Verhinderungseinheit (Vj; j = 1, 2, 3, 4, 5, 6, 7) anzuordnen, mittels welcher Verhinderungseinheit (Vj) im Falle einer unzulässigen Manipulation und/oder eines unautorisierten Zugriffs das Bauelement (200) zumindest partiell deaktivierbar und/oder zumindest partiell zerstörbar ist.

Fig. 1

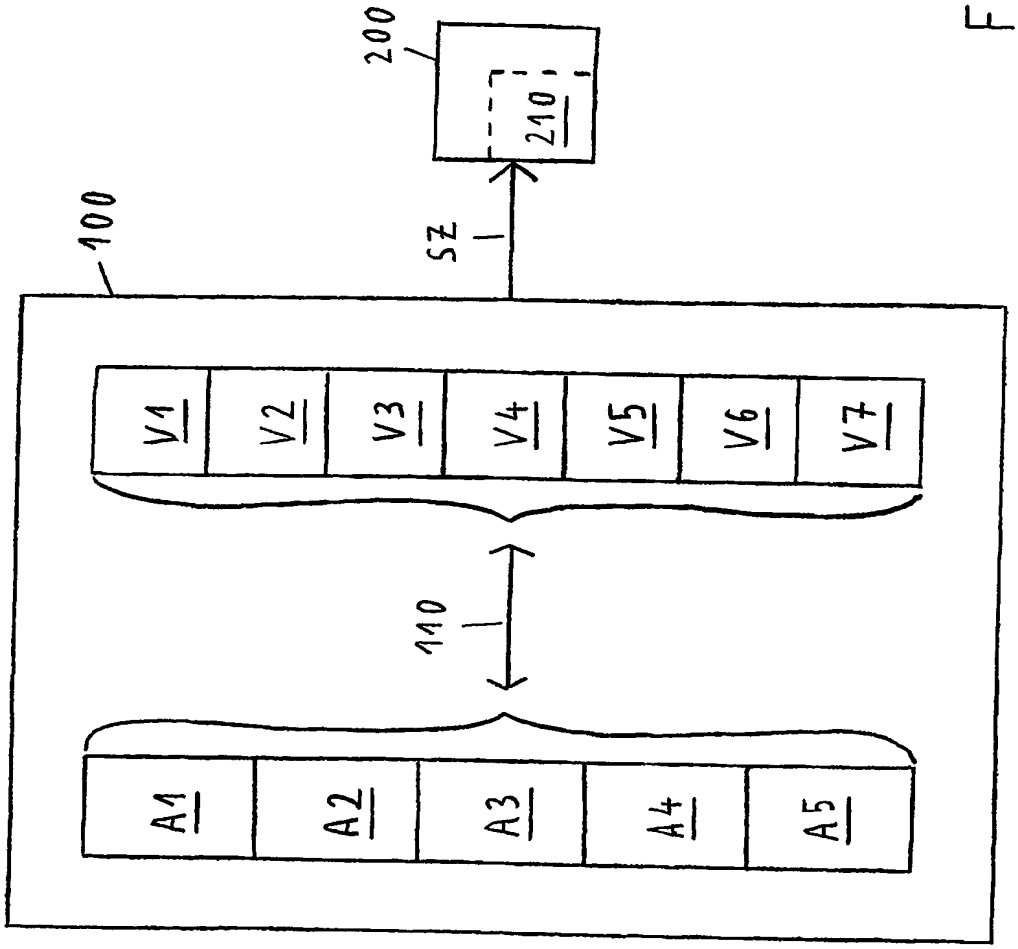

Fig. 1